

Форма № ДН-7.02.1

Державний вищий навчальний заклад
«Навчально-науковий інститут комп'ютерних наук і технологій»
Кафедра Прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

Леонід Бачурін

«19» вересня 2020 р.



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДВС 1.08 Технології захисту інформації

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність: 122 Комп'ютерні науки
(шифр і назва спеціальності)

Освітня програма: Комп'ютерні науки
(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни Технології захисту інформації
(повна назва дисципліни)
для здобувачів вищої освіти за спеціальністю 122 Комп'ютерні науки.

«19» вересня 2020 року. — 4 с.

Розробники: ас. каф. ПМІ Черняк Т.О.

Робоча програма затверджена на засіданні кафедри Прикладної математики та інформатики
(назва кафедри)

Протокол № 11 від «1» травня 2020 р.

Завідувач кафедрою ПМІ д.т.н. проф. Дмитрієва О.А.

(підпис)

Дмитрієва О.А.

(прізвище та ініціали)

«1» травня 2020 р

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології
(шифр, назва)

Протокол № 6 від «7» травня 2020 р.

«7» травня 2020 р. Голова

(підпис)

Башков Є.О.
(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	Вибіркова	
Обсяг в кредитах ЄКТС	6	
Обсяг в годинах за навчальним планом, разом: в тому числі:	180	
лекції:	48	
практичні заняття:	32	
лабораторні заняття:	-	
семінари:	-	
самостійна робота:	100	
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Асистент кафедри ПМІ Черняк Т.О. https://wiki.donntu.edu.ua/view/Черняк_Тетяна_Олександрівна e-mail: tetiana.chemniak@donntu.edu.ua	

Передумови для вивчення дисципліни: теоретичною базою вивчення навчальної дисципліни є такі дисципліни: «Вища математика», «Програмування», «Основи алгоритмізації», «Дискретна математика», «Теорія ймовірностей і математична статистика» та «Чисельні Методи».

2. Мета вивчення навчальної дисципліни

Основними завданнями вивчення навчальної дисципліни «Технології захисту інформації» є набуття теоретичних знань та практичних умінь з формування базового уявлення про галузі застосування технологій захисту інформації. Формування знань і умінь, необхідних для розробки програм, що реалізують алгоритми спеціального кодування інформації. Навчити студентів створювати програми із використанням будь якої мови програмування, що реалізують певні криптографічні алгоритми на рівні бітового представлення даних.

Як результат вивчення навчальної дисципліни повинні бути сформовані наступні компетентності:

- здатність визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг безпеки в ІС та Т;
- здатність ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в ІС та Т;
- здатність забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;
- здатність аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники ІС та Т в цілому.

Як результат вивчення навчальної дисципліни повинні бути сформовані наступні програмні результати навчання:

- основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки ІС та Т;
- основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;
- механізми та протоколи забезпечення конфіденційності ІС та Т;

- механізми та протоколи забезпечення автентичності ІС та Т;
- механізми та протоколи забезпечення цілісності даних ІС та Т;
- модель порушника, основні види атак, принципи криптоаналізу;
- механізми та протоколи керування ключами в ІВК інформаційної системи;
- методи та процедури цифрової стеганографії

3. Очікувані результати навчання

Результати навчання, які базуються на програмних результатах навчання:

- здатність проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів;
- здатність забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій;
- здатність здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності.

4. Засоби діагностики результатів навчання

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Форма проведення поточного контролю – усна бесіда за результатами виконання практичних робіт.

В процесі виконання розрахункової роботи та практичних робіт, студенти досліджують та розробляють програмне забезпечення в галузі захисту інформації. Застосовують методи та алгоритми шифрування та кодування інформації.

Підсумковий контроль проводиться з метою оцінювання результатів навчання та визначається підсумками результатів виконання та захисту практичних робіт по кожному зі змістовних модулів та оцінка розрахункової роботи.

Підсумковий семестровий контроль – екзамен.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Пр.1	Пр.2	Пр.3	Пр.4	Пр.5	Пр.6	Інд.завд.	Поточний контроль	Іспит	Максимальний бал
5	5	5	5	5	5	10	40	60	100

Примітка: Пр.1, Пр.2 і т.д. практичні роботи;
С.1, С.2 і т.д. семінарські заняття;
Лр.1, Лр.2 і т.д. лабораторні роботи.

Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Основні поняття теорії кодування. Міра невизначеності. Інформація. Ентропія. Властивості ентропії. Математичні положення теорії чисел.

Тема 2. Традиційні криптографічні системи. Криптографія і її основні поняття. Модель криптографічної системи. Види історичних шифрів.

Тема 3. Методи оптимального кодування інформації (метод Шенона-Фано, метод Хаффмана).

Тема 4. Захист інформації від завад. Принципи завадостійкого кодування. Різновиди завадостійких кодів.

Тема 5. Коди, що виявляють помилки. CRC-кодування. Коди, що відновлюють помилки. Метод Хемінга.

Тема 6. Базові криптографічні методи. Зворотні математичні функції. Частотний аналіз. Шифрування за методом одноразового блокноту.

Тема 7. Генератори псевдовипадкових послідовностей. Побудова генераторів цілих чисел, дробових чисел та бітових послідовностей. Методи визначення якості генераторів псевдовипадкових послідовностей.

Тема 8. Застосування генераторів псевдовипадкових чисел в криптографії. Метод одноразового блокноту на базі генератора псевдовипадкових послідовностей.

6.2. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Формування таблиць простих чисел Тема 1. Основні поняття теорії кодування. Міра невизначеності. Інформація. Ентропія. Властивості ентропії. Математичні положення теорії чисел.	4	
2	Програмна реалізація класичних алгоритмів шифрування Тема 2. Традиційні криптографічні системи. Криптографія і її основні поняття. Модель криптографічної системи. Види історичних шифрів.	4	
3	Дослідження алгоритмів стиснення інформації Тема 1. Основні поняття теорії кодування. Міра невизначеності. Інформація. Ентропія. Властивості ентропії. Математичні положення теорії чисел. Тема 3. Методи оптимального кодування інформації (метод Шенона-Фано, метод Хаффмана).	4	
4	Шифрування інформації з використанням оборотних математичних функцій Тема 6. Базові криптографічні методи. Зворотні математичні функції. Частотний аналіз. Шифрування за методом одноразового блокноту.	6	
5	Побудова і дослідження генераторів псевдовипадкових чисел Тема 7. Генератори псевдовипадкових послідовностей. Побудова генераторів цілих чисел, дробових чисел та бітових послідовностей. Методи визначення якості генераторів псевдовипадкових послідовностей. Тема 8. Застосування генераторів псевдовипадкових чисел в криптографії. Метод одноразового блокноту на базі генератора псевдовипадкових послідовностей.	8	
6	Шифрування даних на основі базових криптографічних методів Тема 6. Базові криптографічні методи. Зворотні математичні функції. Частотний аналіз. Шифрування за методом одноразового блокноту.	6	
...	Усього годин	32	

6.3. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Основні поняття теорії кодування. Міра невизначеності. Інформація. Ентропія. Властивості ентропії.	10	
2	Традиційні криптографічні системи. Криптографія і її основні поняття. Модель криптографічної системи. Види історичних шифрів.	10	
3	Методи оптимального кодування інформації (метод Шенона-Фано, метод Хаффмана).	15	
4	Захист інформації від завад. Принципи завадостійкого кодування. Різновиди завадостійких кодів.	15	
5	Коди, що виявляють помилки. CRC-кодування. Коди, що відновлюють помилки. Метод Хемінга.	10	
6	Базові криптографічні методи. Зворотні математичні функції. Частотний аналіз. Шифрування за методом одноразового блокноту.	10	
7	Генератори псевдовипадкових послідовностей. Побудова генераторів цілих чисел, дробових чисел та бітових послідовностей. Методи визначення якості генераторів псевдовипадкових послідовностей.	15	
8	Застосування генераторів псевдовипадкових чисел в криптографії. Метод одноразового блокноту на базі генератора псевдовипадкових послідовностей.	15	
	Усього годин	100	

6.4 Індивідуальні та/або групові завдання

Темою розрахункової роботи є дослідження алгоритмів стиснення інформації.

Метою розрахункової роботи є дослідження та використання алгоритмів стиснення інформації. Ручне кодування фрагменту символів рівномірним кодом мінімально достатньої розрядності, рівномірним однобайтовим кодом, методами Шеннона-Фано та Хаффмана.

7. Література

7.1. Основна

1. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368 с.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие. – М.: Логос, 2001. – 264 с.
4. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
5. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

7.2. Допоміжна

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
2. . Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО Компания СМИТ, 2006. – Т. 1. – 292 с
3. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО Компания СМИТ, 2006. – Т. 2. – 252 с.

7.3 Методична

Методичні вказівки до виконання практичних робіт з дисципліни «Технології захисту інформації» (у розробці).

Методичні вказівки до виконання розрахункової роботи з дисципліни «Технології захисту інформації» (у розробці).

8. Інформаційні ресурси

1. Журнал «Информационные технологии. Аналитические материалы» [Электронный ресурс] – Режим доступа: <http://it.ridne.net> – Заголовок з екрану.
2. Історія розвитку інформаційних технологій в Україні [Електронний ресурс] – Режим доступу: http://www.icfest.kiev.ua/MUSEUM/IT_u.html – Заголовок з екрану.
3. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Електронний ресурс] – Режим доступу: www.fbi.gov – Заголовок з екрану.
4. Нормативні акти України [Електронний ресурс] – Режим доступу: www.nau.kiev.ua – Заголовок з екрану.

